SOUTH INDIAN Bank
Experience Next Generation Banking

STUDENTS' ECONOMIC FORUM

To kindle interest in economic affairs...
To empower the student community...

OPEN ACCESS www.sib.co.in
ho2099@sib.co.in

September 2015

Theme 286

INFORMATION SECURITY, ELECTRONIC BANKING, TECHNOLOGY RISK MANAGEMENT & CYBER FRAUDS - PART I

A monthly publication from South Indian Bank

24th Year of Publication

www.southindianbank.com
HOME COME TRUE
WITH SIB HOME LOANS, YOUR DREAM IS EASIER TO REALISE.
LOW INTEREST
ATTRACTIVE TERMS
blackswanindia.com
*Terms & conditions apply

SOUTH INDIAN Bank
Experience Next Generation Banking
The South Indian Bank Ltd., H.O. : 'S.I.B. House', Thrissur, Kerala

SIB STUDENTS' ECONOMIC FORUM

SEPTEMBER 2015

Theme No: 286: Information Security, Electronic Banking, Technology Risk Management & Cyber Frauds - Part I

A well informed customer will make the policy makers as well as organisations which produce goods and services more responsive to the customer needs. This will also result in healthy competition among organisations and improve the quality of goods and services produced.

The "SIB Students' Economic Forum" is designed to kindle interest in economic affairs in the minds of our younger generation. In April 2010 RBI appointed a working group headed by Shri G. Gopalakrishna on information security, electronic banking, technology risk management & cyber frauds. The group submitted its recommendations to RBI in nine broad areas viz. (i) IT Governance (ii) Information Security (IS) (iii) IS Audit (iv) IT Operations (v) IT Services Outsourcing (vi) Cyber Frauds (vii) Business Continuity Planning (viii) Customer Awareness Programmes (ix) Legal Issues.This month we discuss the recommendations of working group

Explain briefly the major recommendations of the working group on IT Governance.
Different banks use different technology & support services. Hence it is not "one-size-fits-all" recommendations

- Each bank should formulate an IT strategy \plan document approved by the board. Each should clearly provide the details of the procedures and guidelines to be implemented and should be reviewed annually
- IT strategy committee consisting of minimum 2 directors as members , one of whom should be an independent director , should be formed at the board level
- There should be a chief Information Officer (CIO) in each bank who should enable the alignment of business & technology
- IT steering committee has to be formed and it should have members from IT field, HR, legal and business functions. IT steering committee should assist the management in the implementation of the board approved IT strategy
- The focus of IT governance should be strategic alignment, value delivery, risk management, resource management & performance management.
- The performance of IT function should be monitored to ensure the delivery on time and within the budget
- There should be proper prioritization and coordination of various IT projects
- For major projects, proper risk assessment should be carried out and to be managed on an ongoing basis.
- There should be a comprehensive management information system well supported by IT.

What are the important recommendations on Information Security (IS) ?

- Each bank should have a separate information security (IS) wing exclusively on information security management.
- A senior level official of the rank (GM\DGM\AGM) should be designated as the chief information security officer (CISO). CISO should report directly to the head of the risk management section and should not have a direct reporting relationship with the Chief Information Officer (CIO).
- Information security policy approved by the board should be there and reviewed at least annually
- Based on the job description , employees can be entrusted with a general and specific security roles and responsibilities
- Personnel with a elevated systems access privileges should be closely supervised
- There should be initial and ongoing training \awareness programmes on information security for employees and vendor personals
- Except in the case of emergency , direct back-end updates to the database should not be allowed

Briefly explain the recommendations on IT Operations

- IT operations include all services which are available to the customers, for example mobile banking, internet banking etc. It also includes IT components which are used to support IT operations.
- Business process, service level agreement, IT infrastructure , IT environment etc. should be considered while designing new IT service or making a change to the existing IT services
- · In order to have an accurate IT landscape, IT service catalogue should be defined and maintained.

What are the main recommendations on IT Outsourcing

- The ultimate responsibility of the outsourced operations and risks involved are with the board and senior management
- Each bank should assess the “materiality” degree involved in the outsource functions
- The bank should evaluate risk factor before entering into an outsourcing agreement and it should be periodically reviewed in the light of known and expected changes
- Appropriate diligence should be done to assess the capability of the service provider during the negotiation \renewing of outsourcing arrangement. All information about the service provider should be collected
- When the scale and nature of function outsources are significant or extensive sharing of data is required, bank must report to the regulator.
- Bank’s advocate\Legal council should vet the agreement which should be written and confirm about the legal effects and enforceability
- The service providers “ limitation of liability” should be properly assessed by the legal department
- The service level agreement(SLA) should be included in the outsourcing agreement
- Pre and post – outsourcing implementation reviews should be conducted by the banks and outsourcing should no way affect the ability of the bank\regulator in performing its functions and objectives
- At least once in a year review should be undertaken about the financial and operational

conditions of the service provider to access the ability of the service provider to continue to meet the outsourcing obligation

- It should be ensured that on account of outsourcing, business continuity preparedness is not compromised
- The bank should take effective steps to ensure that confidentiality and data security are well protected
- IBA may take steps for data sharing between banks regarding any fraud\major operation lapses committed by the service provider

Describe the major recommendations made on Information Security (IS) Audit.

- Considering the complexities involved, adequately skilled audit committee should be formed. There should be at least a designated member of audit committee who should possess knowledge about information system, IS control and audit issues.
- The finding of IS audit should be properly discussed by the audit committee and provide appropriate guidance to the bank management
- Within the internal audit department there should be a separate IS audit section reporting to top chief audit executive (CAE) or head of internal audit. The responsibility and accountability of IS audit conducted by outsourced\outside agency will remain with IS audit head or CAE
- There should be a clear cut audit charter \audit policy well documented containing mandate , purpose, authority and accountability and relevant operative principles approved by the board of directors
- The audit policy should be reviewed annually by the board of directors. IS audit planning should be carried out by the banks using the Risk Based Audit Approach. The IS auditor has to define, adopt and follow an appropriate risk assessment methodology.
- IS audit should cover IT governance, information security governance related aspects, critical IT general controls, Management Information System(MIS) etc
- It should also cover large and medium branches with focus on password control, user ID, operative system security, maker - checker controls, rotation of personals, physical securities etc.
- IS auditor should consider the fraud vulnerability assessment under taken by the fraud risk management group

Recommedations to curb Cyber Frauds

- The frauds should be briefed separately to the special committee of board so that they can review the steps taken by the bank to mitigate them
- The fraud prevention, monitoring, investigation reporting and awareness creation should be carried out and owned by an independent fraud risk management group and it should be headed by a senior official of the bank, not below the rank of GM\DGM
- Fraud risk management group should setup the fraud review council. The council should meet at least once in every quarter to review fraud trends and preventive steps taken.
- Only after the approval of Compliance department and audit department, fraud risk management should introduce or modify products or process
- CIBIL Reports should be used by the banks to collect information about fraudulent accounts
- Banks should setup transaction monitoring group, alert generation and redressal mechanism, dedicated emails, ID and phone numbers for reporting suspected frauds.
- Continuous and special training should be given to the fraud investigation team

Views of the committee on Business Continuity Planning (BCP)

- A senior official should be designated as the head of BCP function
- BCP\crisis management committee consisting of senior officials from the various departments like IT, HR, legal etc. should be constituted
- Banks should consider various BCP methodologies and strategies as inputs for their BCP frame work
- There should be careful understanding of vulnerabilities with the inter relationship between various departments, systems etc.
- The banks must regularly test BCP to confirm that they are effective and up to date
- Internal audit team should audit the effectiveness of BCP and their findings should be incorporated in the report to the Board of Directors, senior management
- Disaster Recovery(DR)\BCP test should be done without movement of special personnal to DR site so that readiness of the alternative staff at the DR site can be tested or checked
- BCP plans should be reviewed at least annually
- Configuration of services, network devices and other product at Data center (DC) and Disaster recovery should be always identical. This is also applicable to the patches that are applied at DC
- DR drill should be conducted periodically

Suggestions to improve Customer Education

- Special care should be taken by the board of directors\senior management for improving customer education measures
- There should be a systematic process for the development of customer awareness programme
- Regular evaluation should be done about the effectiveness of the various customer awareness programme
- Each bank should have a documented policy, training mechanism and research unit on customer education

Working groups views on Legal Issues

- There should be adequate trained staff to address legal issues arising from cyber laws
- There should be a good and efficient system in the bank to track and identify the transaction as per guidelines on AML and report the matter with the allotted time period which will help the institution to avoid the risk of penalty and reputation.
- There is restriction at the level of encryption for the individuals, group or organization to a key length of 40 bits only in symmetrical key algorithm or equivalents. Banks may be allowed for higher encryption
- Attempt to phishing should be made punishable

www.southindianbank.com

YOUR DREAM VEHICLES ARE DIFFERENT. SO ARE OUR VEHICLE LOAN SCHEMES.

TAILORED TO SUIT THE NEEDS OF:

| SALARIED CLASS | BUSINESS PEOPLE | NEXT GEN
| AGRICULTURISTS | NRIs | SENIOR CITIZENS

blackswanindia.com

*Terms & conditions apply

| Low Interest Rates | Easy Processing | Enhanced Eligibility

SOUTH INDIAN Bank

Experience Next Generation Banking

The South Indian Bank Ltd., Regd. Office, SIB House,P.B. No. 28, Thrissur, Kerala, PIN-680 001
Ph: 0487 2420020, Fax: 0487 2426187, Toll Free (India): 1800-843-1800, 1800-425-1809 (BSNL)
Email: sibcorporate@sib.co.in | CIN : L65191KL1929PLC001017

South Indian Bank is a member of BCSBI and is committed to treat customers in a fair, transparent and non-discriminatory manner.

http://www.facebook.com/thesouthindianbank www.southindianbank.com

SHAKE TO TRANSFER MONEY AND DO MUCH MORE.

SIB MIRROR
REFLECTION OF SOUTH INDIAN BANK

Never-before features on a smart banking app:

Shake to transfer funds | Shake to know balance | Click to share your account information | Gesture support for menu access* | Menu navigation using voice recognition* | Pattern lock

OTHER FEATURES

Calculators | Forex Rates | SIB Locator | My Account (only for SIB account holders) | Deposit Rates | Apply for Deposits and Loans | Contact Us | About Us

THE SMART WAY TO BANK WITH SOUTH INDIAN BANK.
DOWNLOAD SIB MIRROR ON YOUR SMARTPHONE NOW.

Android | i-Phone | Windows Phone | Blackberry

*Handset specific

The South Indian Bank Ltd., Regd. Office, SIB House, P.B. No. 28,
Thrissur, Kerala, PIN-680 001, Ph: 0487 2420020, Fax: 0487 2426187,
Toll Free (India): 1800-843-1800, 1800-425-1809 (BSNL),
Email: sibcorporate@sib.co.in | CIN : L65191KL1929PLC001017

http://www.facebook.com/thesouthindianbank

SOUTH INDIAN Bank
Experience Next Generation Banking

South Indian Bank is a member of BCSBI and is committed to treat customers in a fair, transparent and non-discriminatory manner.

blackswanindia.com